Global Counsel

Prospects for US data breach law soar after SolarWinds hack

Blog post by Senior Associate Miranda Lutz, 3 March 2021

The fallout from the SolarWinds hack that compromised a number of US government systems just before the end of 2020 continues to ripple across the US government, with Congress holding three public hearings on the topic in February alone. The SolarWinds cyberattack revealed that parts of the US government are grossly underprepared for cybersecurity attacks. But it has also triggered intense scrutiny of the private sector over what cybersecurity standards companies should meet, and if they have should have the obligation to report breaches to the government.

The type of breach notification standard Congress will pursue is likely to be sweeping. While certain sectors are already subject to some reporting requirements (namely financial services and healthcare), any new data breach notification law would apply to all industries – including Big Tech. Previously, Congress has stated that any business entity "that that uses, accesses, transmits, stores, disposes of, or collects sensitive personally identifiable information" would be required to notify the government and individuals of a breach. This would significantly expand the scope of government oversight into cybersecurity.

Data-breach bills have been introduced in Congress for almost two decades. But historically, these efforts have failed due to two key factors: 1) pushback from the private sector due to concerns that voluntarily coming forward with a breach could hurt their reputation and bottom line and; 2) breach notification requirements are often tied to even thornier arguments over the need for a federal data protection law and states' rights.

The SolarWinds attack appears to have been seismic enough to shift industry's response. Microsoft President Brad Smith has led the charge for a notification law. The hack has also created a sense of urgency from lawmakers to overcome hurdles related to superseding state laws and separating breach notification from data privacy.

There are several big policy questions around what should be included in data-breach notification requirements. Who is subject to the law? What information must be shared with the government and within what timeframe? What government entity will oversee the program? Will companies that report a breach have liability protections?

In a hearing on the SolarWinds attack held on February 26th, Representatives Michael McCaul (R-TX) and Jim Langevin (D-RI) sketched out legislative approaches that would answer some of these questions. Their proposed solution is to protect companies by only requiring private firms to submit specific threat information to the Cybersecurity and Infrastructure Security Agency (CISA). Sources, methods, and names would be excluded from the reporting requirements. Previous iterations of data-breach bills would have required notification to law enforcement agencies such as the Federal

Bureau of Investigation (FBI) and other regulators like the Federal Trade Commission (FTC). There now appears to be broad support to make CISA the main point of contact for cyber breaches.

But there is another option policymakers could consider. Congress could create a new federal entity – similar to the National Transportation Safety Board (NTSB) – focused on cyber. This agency would be responsible for investigating and responding to cyber breaches. This type of entity worked well for improving safety of transportation, but such a structure does not cleanly map on to cyberspace due to the simple fact that there far more attempted cyberattacks each day than there are transportation disasters. Strict thresholds would need to be put into place to delineate what kinds of cyber incidents would fall under this new agency's purview.

The main outstanding political question is how lawmakers will treat liability protections and whether there will be enough support for the McCaul/Langevin approach, which would protect companies being linked to attacks. This is an approach backed by most in the private sector. But certain lawmakers, such as Reps. Katie Porter (D-CA) and Rashida Tlaib (D-MI), have made clear that they want the government to retain some authority to go after private companies for negligence. This dynamic would pose problems for an NTSB-like agency given US law bans the probable-cause findings of NTSB aviation-accident investigations from being used in civil litigation. The lesson here is that some form of liability protection for the companies will be needed for private sector cooperation.

Although under a data-breach notification law, businesses would be subject to additional regulatory requirements, a federal data breach requirement could actually reduce reporting burdens on the private sector. In the US, all 50 states have passed their own form of data breach notification laws. For businesses that operate across multiple jurisdictions this patchwork creates conflicting requirements and obligations. A federal law, that supersedes the states, would create once set of compliance rules for companies.

Congress and administration officials will be dealing with the repercussions of the SolarWinds hack for years to come. But after decades of national debate on whether to pass a federal data breach law, it seems the SolarWinds hack has finally sparked enough momentum to get such legislation much closer to the finish line.